



Nick DePetrillo
Independent Security
Researcher



Don A. Bailey
iSEC Partners, Inc.

WE FOUND
CARMEN SANDIEGO

We know *who* you are.



We know *where* you are.



We know *who* you talk to.



We know *what* you talk about.



Or, at least... we have a good idea ;)

Reference

- Home Location Register (HLR)
- Signaling System #7 (SS7)
- Mobile Switching Center (MSC)
- Mobile Subscriber Integrated Services Digital Network (MSISDN)
- International Mobile Subscriber Identity (IMSI)
- Numbering Plan Area (Area Code) (NPA)
- NXX (Telephone Exchange)

The Goose that Laid the Golden Easter Egg

- What can't you do with SS7 access?
- What *can* you do without it...?
 - Location information
 - Identity information
 - Provider specific attacks

Leveraging location data

Tobias Engel and Mobile Tracking

- Uncovered HLR services in the EU
 - SMS services offering HLR queries
- Services accessible via Web API
- Affects
 - GSM
 - CDMA (not discussed in Tobias' talk)

What do you get for fractions of a cent?

- HLR information on a per-subscriber basis
 - What origin provider?
 - What origin country?

- Marketing “augmentation” data
 - MSC
 - IMSI

Provider? Country? So what!

- Provider (MNC)
 - Maintain stealth during provider specific attacks
 - Allows the attacker to know what network a target is using for “IMSI catching”

- Country (MCC)
 - Allows us to know whether a target is roaming
 - Tells us where the target is from

IMSI, the subscriber's identity

- Unique serial number for a SIM card
- Should never be exposed to someone outside the the network
- Sent rarely as possible
- TMSI is sent instead (Temporary IMSI)
- Knowing the IMSI allows tracking and interception

Ah, so that's what that means..

- MSC values equate to a physical location
- With *varying* granularity
- Switching center may span *multiple* cities
- May only exist in *one part* of a city
- However, MSC values for the USA must be reverse engineered
- ...and they can be

Mapping the MSC

- NANPA is our Friend
- NPANXX database describes...?
 - Area Codes
 - Exchanges
 - What state
 - What rate center (essentially, the city)
 - What company has been allocated that NPANXX

Mapping the MSC

```
root@mail:~
mysql> SELECT * FROM npanxx_lookup WHERE ratecenter LIKE '%denver%' AND company LIKE '%mobile%';
```

id	state	npa	nxx	ocn	company	ratecenter	effectivedate	npanxx_use	assigndate
22893	CO	303	332	6529	T-MOBILE USA, INC.	DENVER		AS	
22920	CO	303	359	6529	T-MOBILE USA, INC.	DENVER		AS	
23084	CO	303	523	6529	T-MOBILE USA, INC.	DENVER		AS	
23125	CO	303	564	6529	T-MOBILE USA, INC.	DENVER		AS	
23228	CO	303	667	6529	T-MOBILE USA, INC.	DENVER		AS	
23229	CO	303	668	6529	T-MOBILE USA, INC.	DENVER		AS	
23230	CO	303	669	6529	T-MOBILE USA, INC.	DENVER		AS	
23436	CO	303	875	6529	T-MOBILE USA, INC.	DENVER		AS	
23492	CO	303	931	6529	T-MOBILE USA, INC.	DENVER		AS	
23521	CO	303	960	6529	T-MOBILE USA, INC.	DENVER		AS	
24053	CO	720	217	6529	T-MOBILE USA, INC.	DENVER		AS	
24056	CO	720	220	6529	T-MOBILE USA, INC.	DENVER		AS	
24067	CO	720	231	6529	T-MOBILE USA, INC.	DENVER		AS	
24074	CO	720	238	6529	T-MOBILE USA, INC.	DENVER		AS	
24096	CO	720	261	6529	T-MOBILE USA, INC.	DENVER		AS	
24115	CO	720	280	6529	T-MOBILE USA, INC.	DENVER		AS	
24131	CO	720	299	6529	T-MOBILE USA, INC.	DENVER		AS	
24153	CO	720	323	6529	T-MOBILE USA, INC.	DENVER		AS	
24168	CO	720	341	6529	T-MOBILE USA, INC.	DENVER		AS	
24178	CO	720	352	6529	T-MOBILE USA, INC.	DENVER		AS	
24203	CO	720	394	6529	T-MOBILE USA, INC.	DENVER		AS	
24207	CO	720	401	6529	T-MOBILE USA, INC.	DENVER		AS	01/13/2009
24213	CO	720	421	6529	T-MOBILE USA, INC.	DENVER		AS	03/20/2009
24312	CO	720	771	6529	T-MOBILE USA, INC.	DENVER		AS	
24378	CO	720	933	6529	T-MOBILE USA, INC.	DENVER		AS	
24379	CO	720	934	6529	T-MOBILE USA, INC.	DENVER		AS	
24380	CO	720	935	6529	T-MOBILE USA, INC.	DENVER		AS	
24381	CO	720	936	6529	T-MOBILE USA, INC.	DENVER		AS	
24382	CO	720	937	6529	T-MOBILE USA, INC.	DENVER		AS	
24383	CO	720	938	6529	T-MOBILE USA, INC.	DENVER		AS	
24384	CO	720	939	6529	T-MOBILE USA, INC.	DENVER		AS	

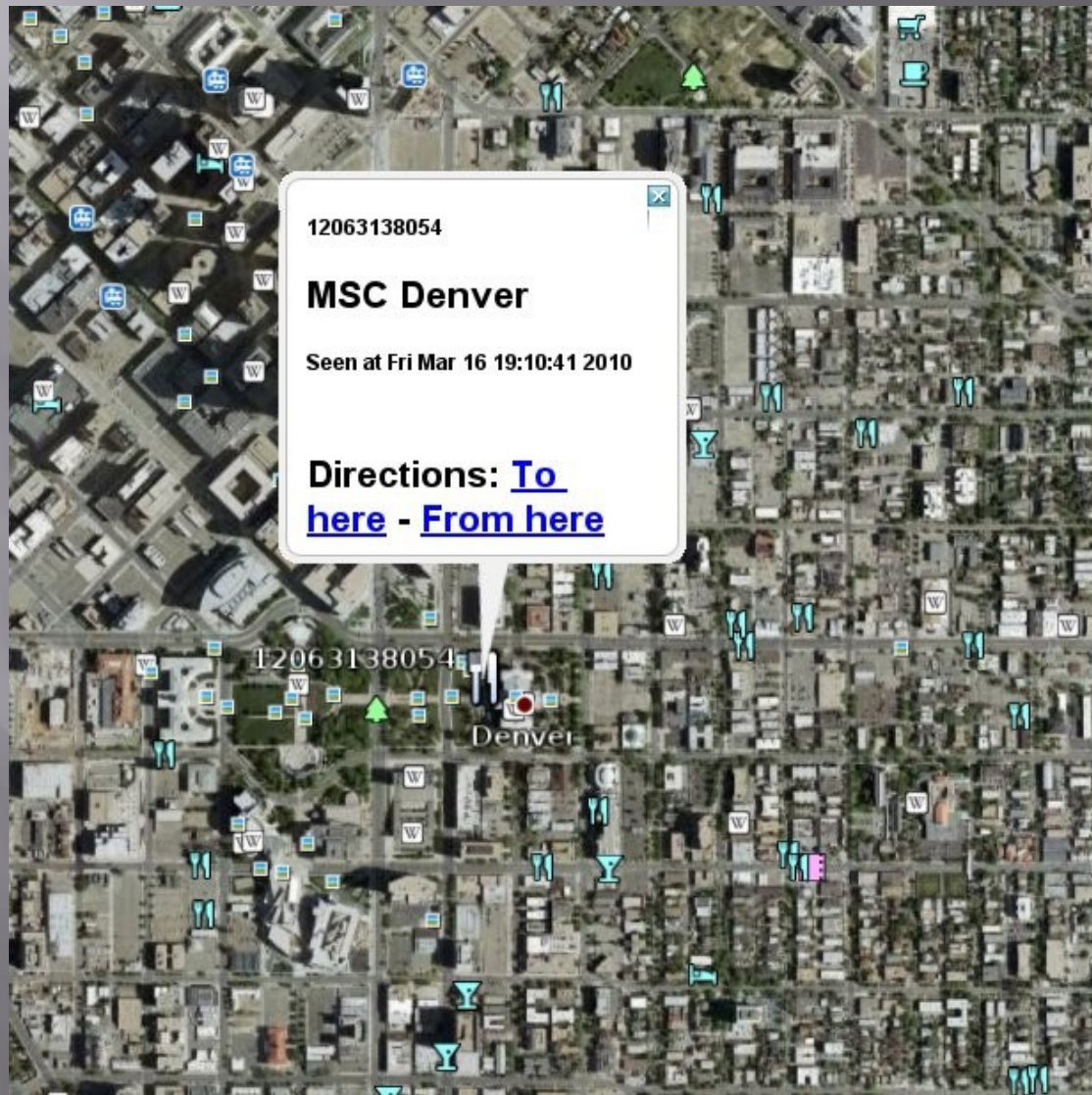
```
31 rows in set (0.11 sec)

mysql>
```

Mapping the MSC

- Query the HLR APIs for MSC data for each subscriber
- Pick logical times when most people are not mobile
 - Early morning
 - Afternoon
 - Late evening
- Correlate the resulting data

Mapping the MSC



Mapping the MSC

- Enhance the location information by creating bounding boxes
- How? Define who a subscriber is...
- Okay... so how?

Who are you?

White pages for cellphones?

- Not a public resource, but not a private one, either.
- CNAM service is all you need
- A VoIP line enhanced with CNAM = Win

But wait... how do you get the victim to call you?

- We need to?
- Caller ID spoofing and time is all you need.
- Fractions of a cent.
- Line receiving the call simply logs the CNAM record and drops the call.
- Answering the line isn't necessary.

root@mail:~

```
mysql> SELECT * FROM cnam_lookup WHERE cnam LIKE '%emb%' OR cnam LIKE '%govt%' OR  
cnam LIKE '%trac%' OR cnam LIKE '%shell%' OR cnam LIKE '%wits%' OR cnam LIKE '%p  
aragon%' OR cnam LIKE '%moore%h%';
```

id	date	num	cnam
1284	2010-04-19 03:18:02	617	MOORE RICHARD
1410	2010-04-19 13:16:28	303	MOOREJOHN
2315	2010-04-19 17:00:38	407	SATELLITE TRACK
2363	2010-04-19 17:05:26	407	SATELLITE TRACK
2413	2010-04-19 17:10:00	407	SATELLITE TRACK
2435	2010-04-19 17:11:48	407	SATELLITE TRACK
2461	2010-04-19 17:13:57	407	SATELITE TRACKI
2463	2010-04-19 17:14:08	407	SATELLITE TRACK
2571	2010-04-19 18:48:47	202	EMBASSY OF UKRA
3887	2010-04-19 23:52:46	713	SHELL COMPANIES
3888	2010-04-19 23:52:52	713	SHELL COMPANIES
3889	2010-04-19 23:52:58	713	SHELL COMPANIES
3891	2010-04-19 23:53:11	713	SHELL COMPANIES
4187	2010-04-20 00:18:48	713	US GOVT F B I
4203	2010-04-20 00:19:33	713	US GOVT F B I
4489	2010-04-20 21:03:48	202	WITS3
4490	2010-04-20 21:04:12	202	WITS 2001
4492	2010-04-20 21:05:03	202	PARAGON SYSTEMS
4501	2010-04-20 21:07:46	202	WITS 2001
4529	2010-04-20 21:13:23	512	MOOREH

20 rows in set (0.01 sec)

```
mysql> █
```

Back to NPANXX

- Pull the NPANXX records by region and company
- Build a profile of subscribers for that region
- Are lots of MSISDNs 'Unavailable'?
- Are they people?
- Are they businesses?
- Are they organizations? (Government/etc)

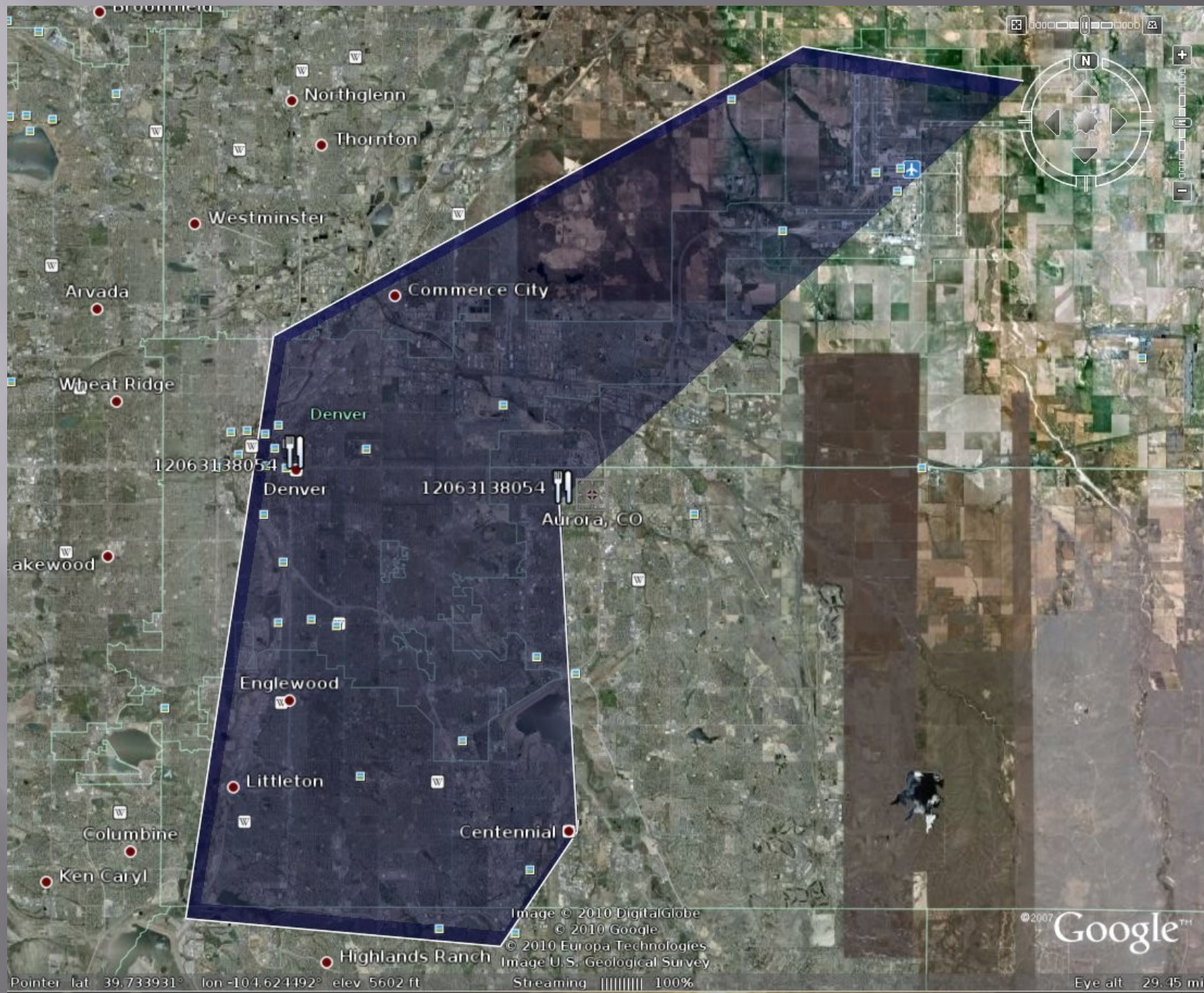
The White Pages

- White Pages now provides a web API
- Search by name and city/state
- Rate Center (NPANXX) + State + Caller ID = Win
- Some records will hit
- Records with addresses contain geo-location data!

Tying HLR and Caller ID Together

Bounding Boxes for MSCs

- Not only do we know who you are, but ...
- Now we can enhance our MSC map with geo-location data
- Creates a sort of bounding box for MSCs
- Note that this will change over time



Pointer lat 39.733931° lon -104.624492° elev 5602 ft

Image © 2010 DigitalGlobe
© 2010 Google
© 2010 Europa Technologies
Image U.S. Geological Survey
Streaming 100%

© 2007 Google™

Eye alt 29.45 mi

Understanding MSC Boundaries

- Enhances the ability for an attacker to perform IMSI catching
- If they are watching you move from MSC to MSC, they can make approximations of your location
- But, don't they have to compete with the actual cell towers?
- Yes. But... there's a database for that (:

OpenCELL ID

What is OpenCELLID?

- Database provides
 - Cell tower location information
 - Latitude
 - Longitude
 - What provider owns or leases that tower
 - MCC
 - MNC

What is OpenCELLID

- Allows us to infer
 - What set of potential cell towers a subscriber will land at on a MSC transfer
 - Where the cell towers are in relation to
 - The attacker
 - The potential locations for a target handset

Competing for Strongest Signal

- Results in enhanced IMSI Catching
 - Make predictions about which cell tower you will associate with next
 - Based on travel (MSC) data changing over time
 - Provides the attacker with enough ammunition to compete with higher probability of success

Tying together MSC, CallerID, White Pages and OpenCELLID

Now we know...

- Where you are
- Who you are
- Where your MSC boundary lies
- What cell towers you're likely on in that MSC
- What subscriber you are within that cell

Paranoid yet?

Provider specific attacks

You know voicemail is a problem. Don't you?

- Ye old Caller ID spoofing trick
- Snoop on someone's Voice Mail with ease
- Change their VM announcement to Rick Astley

Wait, guys! That's old news!

Pulling provider HLR data in...

- Knowing the provider enhances stealth
- Maximize success of attack while minimizing exposure
- Allows for provider specific attacks, such as...
 - Knowing whether the network allows certain types of SMS messages
 - Allows tailoring of SMS/MMS specific attacks
 - Whether caller ID spoofing may lead to voicemail breakins

Well, sure. But info is 1nf0, yo!

- Let's talk about voice mail crawling.
- Extract phone numbers from voicemails that have been left
- Pull Caller ID records on those phone numbers
- Pull location data on those phone numbers
- It's not just ASM's social network research!
- We can...
 - Make relationship associations using tracking data
 - Predict patterns of behavior in social groups, not just individuals

Behavior based triggers

- What if you notice behavior patterns change using location and VM data?
- What if suddenly
 - A husband and wife are at different locations during the evening according to MSC?
 - A co-worker is no longer in the same location data during the afternoon?
 - Two executives meet at regular monthly intervals at some location

Behavior based triggers

- Curious about what's happening?
- Leverage ASM's LOLphone (Toorcon 2007)!
 - Swaps Caller ID for two victims
 - Drop two or more people into a conference with the attacker (or an automated system) snooping the call
 - Catalogue the resulting call
 - Intel enhancement
- What if we connect a victim to her own voice mail box?

Result?

- Opportunistic espionage based on pattern analysis
- Information gathering on groups of individuals
- Ability to ascertain relationships
 - Family
 - Friends
 - Coworkers
 - Executives in Corporations
- Sabotage

**Tying together HLR, Caller ID, White
Pages, OpenCELLID, and Provider
specific attacks**

Now we know...

- Who you are
- Who your friends/family/co-workers are
- Where you are
- Where *they* are
- What you're probably doing
- Why
- ...and what you'll probably do next



Like a 27 inch Zenith, believe it

- We know where you are, but where are your sensors and your SCADA?
- Device profiling? We can do it!
 - Kindles
 - Tracking Devices
 - Urban Traffic Systems
 - SCADA sensors
 - Smart meters
- Coming soon to a conference near you...!

What about CDMA?

- The Answer is NOT 42
- ...it *is* 41
- Yes... we are working on CDMA!
- Coming soon to a conference near you!

Thanks to the special few

- Bernard Abbott
- Jake Appelbaum
- Kevin Bankston
- Jesse Burns
- Joe Conlin
- Jennifer Granick
- Mike Kershaw
- HD Moore
- Karsten Nohl
- Chris Paget
- Chris Palmer
- Tyler Shields
- Josh Wright

Questions?

```
root@mail:~#  
mysql> SELECT id, num, cnam FROM cnam_lookup WHERE cnam LIKE '%sand%carmen%';  
+-----+-----+-----+  
| id    | num          | cnam          |  
+-----+-----+-----+  
| 4535  | 127.0.0.1    | SANDIEGOCARMEN |  
+-----+-----+-----+  
1 row in set (0.00 sec)  
  
mysql> █
```

